Written Testimony of Mari J. Frank, Esq.
For the Senate Judiciary Subcommittee on Terrorism, Technology, and Government Information on:
"Local and Federal Response to Identity Theft"
Wednesday, August 30, 2000
4700 Ramona Blvd., Monterrey Park California

Senator Feinstein and honorable members of this committee, thank you for the opportunity to address you today. In May of 1998, I appeared before this distinguished committee when you considered the Identity Theft and Assumption Deterrence Act of 1998. I especially applaud Senator Kyle and Senator Feinstein for their leadership and efforts in the passage of that law. By making Identity Theft a federal crime, it helped to educate states to also make Identity theft a crime. We now have almost 40 states that have enacted statutes-only Arizona had a statute when I became a victim. The federal legislation also established a central clearinghouse for identity theft complaints within the Federal Trade Commission. There is now a toll free number for consumers to call (1-877-IDTHEFT) and a web site of information at www.consumer.gov/idtheft.. I am grateful that congress focussed on law enforcement's role and allocated more resources, and I am pleased that the Federal Trade Commission is providing education to victims *after* they find out about their evil twin, but that Act did nothing to *prevent* the crime from occurring.

When I testified on that bill, I brought to your attention how the credit reporting agencies and the credit grantors were facilitating the crime of identity theft. I demonstrated how certain practices in the financial industry made the social security number easily accessible to fraudsters (it is the key to identity theft), and continued with procedures that failed to verify identity and address changes. Thank you for listening to those concerns and addressing those issues in Senate Bill S2328,

The Identity Theft Protection Act of 2000, and in Senate Bill S 2699 The Social Security Number Protection Act of 2000. In my testimony today, I will tell you about real life examples that clarify the need for these bills that you are now considering.

My written testimony will give you a brief overview of my own identity theft nightmares; provide you with insights that I have gained after hearing from thousands of victims; indicate why the bills we are considering today are so critical; share a few helpful tips for consumers to protect themselves, and provide some measures to take if one's identity is stolen.

I am an attorney, the author of The Identity Theft Survival Kit (Porpoise Press, 1998), Privacy Piracy (Office Depot 1999- co-authored with Beth Givens, the Director of the Privacy Rights Clearinghouse), and an Orange County, California Sheriff Reserve for the High Tech Crime Unit. My expertise in Identity Theft was acquired by necessity. In restoring my own life, I was compelled to assist in the passage of state and federal legislation, and create materials to help other victims. Because this epidemic grew so rapidly, those of us who have an understanding of the crime and its causes have been called upon to speak to the media, assist governmental agencies, and provide education to the financial industry and law enforcement. I was greatly honored to address members of congress and the financial industry on May 4 1999, when I spoke at the White House on Consumer Privacy. I shared my story and offered solutions.

In August 1996, I received a call from a bank I that I had never heard of asking me to pay an $11,0000 bill to them. I was about to hang up, when the woman asked if she had my correct social security number, birth date and other identifying information. Upon hearing her tell me my personal and financial information, my heart leaped into my throat. I asked where the company had sent the credit card and billing statements. She gave me an address four hours from my home in a city I had never been. I found out that my impostor had used my credit to obtain all new

credit cards, credit lines, services, and cash advances of over $50,000. She also had purchased a red convertible mustang using my name, had rented a car and totaled it and I was being sued by the rental car agency. My impersonator was also assuming my professional identity by using my name on business cards indicating that she was a licensed California attorney.

It took me over 500 hours and more than 10 frustrating months to regain my credit- I have 5 overstuffed bankers boxes filled with correspondence with credit reporting agencies, credit card companies, the IRS, the Social Security Administration, the Postal Inspector, the State Bar of California, and on and on. In 1996, according to state law and federal law I was not considered the victim. Until I found a peace officer that was a victim himself, I could not get a police report. Even though there are almost 40 states with Identity Theft statues, over half of the victims who contact my office cannot get law enforcement to issue a report. Many law enforcement agencies are concerned that if a report is issued, a full investigation will be needed, and there are just not enough resources to investigate all the identity theft. Unfortunately, without a police report – it is impossible to clean up the mess. Although prior to my stolen identity, I had pristine credit, after my evil twin abused my financial profile, I was considered a low life that didn't want to pay my bills. I was hounded by creditors and collection agencies and ignored by the Credit Reporting agencies. Victims call me every day telling me the same story.

I found out that my" identity clone"- who I never knew, had been working as a contract secretary in several law offices. She was able to access a copy of my credit report as well as those of other victims. Many law offices as well as car dealerships, realtors, banks, etc. have on line or fax subscriptions to order credit reports from the credit reporting agencies and resellers. So my impostor accessed the system, obtained my entire personal and financial profile, including my social security number, and took over my identity. Because I was tenacious, and the law enforcement agency in the city where she resided had empathy, she was arrested. Soon after she was released on bail, she continued to defraud others and me. She

stalked my family by phone; dumpster dived my garbage, stole my mail, and still drove around in the red convertible mustang purchased with my credit. A year later she was sentenced to a two month work furlough program and probation (still driving that car). A few months later she was apprehended committing identity theft again in a different state. Unfortunately, although the police took the case seriously, the district attorney and judge saw this as economic crime- the stepchild of the criminal justice system. Very few of identity theft cases are investigated- thus few impostors are prosecuted unless there is a great loss or a crime ring is involved.

Although I was victimized, I chose not to succumb to victim-hood. I created the kit that I wish I would have had- The Identity Theft Survival Kit with pre-written legal letters on diskette and step by step instructions. I developed a web site with over 70 pages of free information to help other victims. Because of this outreach to victims, I receive at least 100 e-mails and call a month from victims and frightened consumers across the country. They are still experiencing the same problems with financial industry as I did.

Before I go into those problems and how the two bills presented help focus on those concerns, it is important to know that no one is immune from this crime and that it can happen more than once to the same person. I receive calls from lawyers, doctors, homemakers, retired persons, teachers, students, judges, and even widows who tell me that their loved one who has died is a victim after death.

In early July, 2000 (last month) I gave a presentation on Identity Theft for Chase Manhattan Bank in New York City. I explained to them how a customer can become a victim of identity theft from "skimming" when, for example, a waiter takes a credit card at the end of the meal, slides the card through a small 3" by 5" skimmer in his pocket, then processes the card at the register and returns the card to the cardholder smiling and gratefully accepting his tip. That evening, the fraudster downloads the information that he obtained from the back of the

customer's card and sends it to make a new card with the duplicated metal strip of the customer's card on the fraudulent card.

When I returned to California after the program, I opened my American Express bill to find over $9,000 of fraudulent charges with my credit card still in my wallet. Cleaning this mess only took me 7 hours. Amex promptly opened an investigation, but told me that they would not notify me of the results. They gave me the telephone numbers of the two car dealerships (where most of the fraud occurred) located in a California city that I had not visited. Upon calling the dealerships, I learned that the *man* who used my "card" was named Michael Brown and he lived at an address near the dealerships several hours from my residence.

So here I was- victimized again. I called the fraud department of the three credit reporting agencies. After at least twenty minutes of pushing buttons and waiting, I finally was able to reach a human at Equifax and TransUnion. They told me to write to them concerning the fraud enclosing copies of my license and a utility statement. Within a week I received my credit reports- the fraud departments of those agencies provided no further referrals, assistance or suggestions. I fortunately knew what steps to take; however, most victims haven't a clue of what to do!

When I called Experian, even after pushing every button on my phone, I could not reach a live person. I was told by recorded message that I was to send a letter referring to my fraud and I would receive a report within 10 days. After 20 days I received a form letter- just last week, stating that I needed to send $8.00- when in fact a credit report is free for victims of fraud. I had sent my mortgage statement, acopy of my driver's license and a utility bill. After a call to the number on the form letter, I waited 30 minutes until I received a live, but rude person who told me that I needed to send a recent phone bill to get my report and place a fraud alert on my file for more than 90 days-up to seven years. After demanding to speak to a supervisor, I was allowed to fax the phone bill, and he agreed to send my credit report by overnight mail once he found out I was to testify at this hearing. Most

victims are overwhelmed when they call the credit bureaus. They don't know what to ask for and receive virtually no assistance or reassurance from the credit reporting agencies. Although the Credit Bureaus claim that they have improved their assistance, my experience just this month, and the e-mails and phone calls I receive, tells me otherwise.

When I became a victim the first time, it was a total identity take over, obviously much worse than this recent skimming incident. - My evil twin took advantage of a very easy system, which is illustrated by the attachments to this written testimony. My convicted impostor, Tracey Lloyd had received a promotional offer sent to her residence by The Bank of New York, Delaware. This started the "identity cloning " process. You can see from this document, that she crossed one line through her name, inserted mine, wrote in my social security number (which I have erased for obvious reasons) and added some other identifying information, much of which was *not correct,* and within two weeks she received a credit card at her address with my name with a credit limit of $10,000.

Whose fault was it that Tracey Lloyd was able to commit fraud?
Why didn't the bank's personnel question the fact that the name associated with the address was crossed out and changed to an entirely different name on the application? Clearly the bank pulled my credit profile before issuing a card with such a $10,000 credit limit. Why did the bank issue the credit card to an address that was different from the address on the my credit report? Why didn't the bank question the fact that the name of the law office and the address on the application did not match the information on my credit report? If the bank had taken just a moment to verify and match, they would not have issued the card without further investigation- Because of their faulty procedures, I experienced identity theft hell!

Once the credit reporting agencies get news of a new credit card and a new address, they report the new address as the "current address" even though it may a fraud address. In my case- and this still happens to thousands of victims each day- the

new address was reported to the three agencies. This activity of a new card prompted the agencies to sell my name with the new address on promotion (I have since removed my name from the promotional lists by calling 1-888-5-OPTOUT). Then as you can see in exhibit two attached, my impostor received dozens of *pre-approved offers*- (like candy to her door!) This offer from Security Pacific enabled her to get checks with a $15,000 credit line. The more credit cards she received, the more credible she was, and the more she could apply for. With my business cards and a false driver's license with her picture, she was transformed into a credit worthy professional with instant credit, while my reputation was being destroyed without my knowledge. She had been impersonating me for 11 months before I received that fateful call demanding money. Most victims don't' find out about the identity fraud until they are denied credit or employment or a service. Other times they learn about the fraud when they receive a call from a bank or collection agency. Because of the insidious nature of this crime and the less than careful procedures of the credit grantors and credit reporting agencies, there is little a savvy consumer can do to avoid it if an impostor wants to strike.

For that reason, the Identity Theft Protection Act of 2000- S 2328 provides some important safeguards.

<u>Address Changes</u>

In almost every case in which there is an identity takeover (not skimming or the use of a stolen valid credit card), there is *always* a change of address by the impostor, Holding creditors and credit reporting agencies accountable for verifying address changes is necessary to *prevent* fraud.

The Act requires verification of address for:

1. **Impostors who try to change the addresses for valid cards held by the victim or for potential impostors who try adding their names as additional cardholders at a different address.**
2. **Potential new accounts by persons who apply for cards at a different address than the address listed for the consumer on his credit report.**

<u>Fraud Alerts</u>

A fraud alert provides notice to creditors that the consumer must be called before credit is issued. It is a protection from impersonators opening new accounts without the victim's knowledge. In many cases, even with a fraud alert, credit is issued- especially instant credit where a creditor only receives a credit score and does not see the alert. Also, hundreds of victims have told me that apartments, cell phones, and mortgages were issued in their names *after* a fraud alert is on file with the credit reporting agencies.

Credit reporting agencies will place a fraud alert on the file for 90 days unless the victim takes extra measures to keep the fraud alert on for 7 years. I believe it should be kept on permanently if the victim so wishes; however that is not permitted by the Credit Reporting Agencies.

S 2325 by Senators Feinstein, Kyle and Grassley allows a consumer to place a fraud alert on a file, and requires that this alert be provided to *all* users who access the credit report. More importantly it provides penalties for creditors who extend credit without contacting the consumer to verify if credit was requested. If an impostor obtains credit after a fraud alert is on the file there would be sanctions allowable.

<u>Duty to Investigate and the issuance of Free Credit Reports</u>

Identity theft victims and non- victims who are harmed by merged and mixed files (one consumer's bad credit appears on that of another with a similar name), there are disastrous results and ruined reputations. The best way to ascertain stolen identity (or other errors reducing a consumer's credit reputation) is to see one's credit report Several states have already enacted laws to provide one free credit per year to consumers. All consumers should be able to review their credit reports at no cost once a year to reduce the cost of fraud.

<u>Selling personal information including Social Security Numbers</u>

Presently Credit Reporting Agencies are selling the credit header information to information brokers. The information includes personal identifying information

such as the social security number. This number is the only identifier an impostor needs to steal your identity. We know of consumers who became victims when only their social security number was used- not even their correct name. Consumers right now do not have the right to opt-out of this information being sold. They only have the right to limit their financial profile from being sold without their permission. With no control over the sale of that personal information, on-line brokers are selling the social security number for as little as $20. This is a small investment for criminals who intend to use the information to defraud someone of thousands of dollars.

Individual Reference Services- Disclosures

We are seeing a dramatic rise in cases of criminal identity theft. This occurs when an impersonator is arrested or convicted of a crime in the name of a victim. A victim of criminal identity theft often doesn't even find out about the fraud until he is arrested or denied some benefit. We have helped victims who were denied employment due to criminal records that did not belong to them. Victims have been terminated from their jobs, lost custody of their children, been deported, lost their professional license, etc. Even when we finally ascertain the records and provide fingerprints and mug shots to clean up the criminal records, the information brokers have sold that information dozens of times to entities- so the information continues to proliferate. Presently, many of these victims cannot find out what information was sold, to whom it was sold, how to correct it and how to stop it from being sold erroneously again by others. This type of identity theft can last a lifetime and destroy a person's reputation forever.

S2328 addresses the need to hold the Individual Reference Services accountable. This bill would ensure that consumers could access the information compiled by the various information brokers to see if the information is correct. I suggest that the bill be amended to clarify the correction procedure and provide penalties for failure to correct in a timely manner. Presently I am helping a victim who has cleared his

criminal records, yet the Individual Reference Service company claims it cannot provide a list of who purchased and received the erroneous information so that we can correct the file. This victim was unable to get employment until his story was told on Dateline NBC this past April, 2000.

<u>Summary of Problem:</u>

We are living in an easy credit society (11 Billion pre-approved offers were sent out in 1999), where information is readily transferred in a nano-second on the Internet and that information is worth more than currency. In a matter of a few minutes, an impostor can purchase your social security number and apply for numerous credit cards on-line without your knowledge. The impersonator can get medical care, become a legal citizen, take over your professional status, steal money from your accounts, buy life insurance in your name, purchase a home and even be arrested with your identity. *Anything* you can do- your impersonator can do – We have even had victims tell us that ex- spouses have had friends assume their identity just to ruin their reputation.

So on a local and federal level; we need to work collaboratively. A victim in California may have an impostor in New York City who then sells the data to another criminal in Miami. The impostor could be part of a fraud ring using the mails, selling social security numbers, stealing identities in the workplace through the human resource departments or payroll departments. The crime is complex *after* it occurs. However if all businesses were more conscientious concerning the proper handling of our personal information, and were held accountable to safeguard that data with monetary sanctions, perhaps the situation would change. If the financial and governmental entities were required to verify and authenticate identities (before issuing credit or providing services, or booking criminals) our identity theft problem would be greatly reduced.

PROTECTING YOURSELF

No one can assure you that you won't become a victim since your information and the issuing of credit is beyond your control, however you can minimize your risk by:

1. **Ordering your three credit reports from Equifax, TransUnion, and Experian twice a year to look for fraud accounts and inquiries, and mixed files with errors. Immediately correct anything suspicious and place a fraud alert on your file.**
2. **Shredding or disposing of all of your confidential information off line and on-line. Also shred confidential information in your computer and by using shredding software.**
3. **Don't give out personal information over the Internet or by filling out warranty information. Your personal information is the key especially your social security number. Don't give out your social security number unless it is for some tax purpose. Ask for an alternative number. Presently companies can ask for your social security number, but you don't have to give it- they may deny you service**

For more free information go to www.identitytheft.org**;** www.privacyrightrs.org**; and** www.consumer.gov/idtheft**.**

DEALING WITH IDENTITY THEFT IF IT HAPPENS TO YOU

If you become a victim, go to the above web sites for specific guidelines, but here are the top three things to do:

1. **Immediately contact the fraud department of the three credit reporting agencies to place a fraud alert and obtain your full reports at no charge. Carefully read these reports and identify false names, fraud addresses, fraud inquiries, and fraudulent accounts. (See the free form letter at** www.identitytheft.org **)**

2. **Once you receive your credit reports, make a police report listing all the fraud found on the credit reports and send a copy of the police report with a cover**

letter to each of the credit reporting agencies requesting that all the fraud accounts listed on the police report be removed within thirty days.

3. **Write to all the fraudulent credit grantors (get the addresses from the Credit Reporting Agencies), your own credit grantors and banks to inform them of the fraud and get new passwords (never use your mother's maiden name), write the IRS, the Social Security Administration, the Postal Inspector, etc. (see the list of letters to write at www.identitytheft.org – The Identity Theft Survival Kit has all the letters on diskette and includes step by step instructions for who to call, what to say, and how to get what you need to regain your life.**

Thank you all for the opportunity to testify about the multifaceted issues of identity theft. California is leading the states in number of identity theft reports and has also taken a lead in dealing with proposing solutions. As a former victim and an advocate, I am grateful for your legislative proposals and will be happy to provide you further information and assistance.

Mari Frank